

J002 REGD PCT/PTO 03 APR 2002

TRANSMITTAL LETTER TO THE UNITED STATES  
DESIGNATED/ELECTED OFFICE (DO/EO/US)  
CONCERNING A FILING UNDER 35 U.S.C. 371

AZSI-P-010

U.S. APPLICATION NO (If known, see 37 CFR 1.5

10/089756

INTERNATIONAL APPLICATION NO.

PCT/US00/27584

INTERNATIONAL FILING DATE

04 OCTOBER 2000

PRIORITY DATE CLAIMED

15 OCTOBER 1999

TITLE OF INVENTION

SECURE MULTI-APPLICATION CARD SYSTEM

APPLICANT(S) FOR DO/EO/US

AJIT K. ZACHARIAS

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1. ☐ This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371.
2. ☐ This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S.C. 371.
3. ☒ This is an express request to begin national examination procedures (35 U.S.C. 371(f)). The submission must include items (5), (6), (9) and (21) indicated below.
4. ☐ The US has been elected by the expiration of 19 months from the priority date (Article 31).
5. ☒ A copy of the International Application as filed (35 U.S.C. 371(c)(2))
  - a. ☐ is attached hereto (required only if not communicated by the International Bureau).
  - b. ☐ has been communicated by the International Bureau.
  - c. ☒ is not required, as the application was filed in the United States Receiving Office (RO/US).
6. ☒ An English language translation of the International Application as filed (35 U.S.C. 371(c)(2)).
  - a. ☐ is attached hereto.
  - b. ☒ has been previously submitted under 35 U.S.C. 154(d)(4).
7. ☒ Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371(c)(3))
  - a. ☐ are attached hereto (required only if not communicated by the International Bureau).
  - b. ☒ have been communicated by the International Bureau.
  - c. ☐ have not been made; however, the time limit for making such amendments has NOT expired.
  - d. ☐ have not been made and will not be made.
8. ☐ An English language translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371 (c)(3)).
9. ☒ An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4)).
10. ☐ An English language translation of the annexes of the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371(c)(5)).

## Items 11 to 20 below concern document(s) or information included:

11. ☐ An Information Disclosure Statement under 37 CFR 1.97 and 1.98.
12. ☐ An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.
13. ☒ A **FIRST** preliminary amendment.
14. ☐ A **SECOND** or **SUBSEQUENT** preliminary amendment.
15. ☐ A substitute specification.
16. ☐ A change of power of attorney and/or address letter.
17. ☐ A computer-readable form of the sequence listing in accordance with PCT Rule 13ter.2 and 35 U.S.C. 1.821 - 1.825.
18. ☐ A second copy of the published international application under 35 U.S.C. 154(d)(4).
19. ☐ A second copy of the English language translation of the international application under 35 U.S.C. 154(d)(4).
20. ☐ Other items or information:

100-440302  
JC10 Rec'd PCT/PTO 03 APR 2002

**CALCULATIONS PTO USE ONLY**

\$ 890.00

\$

\$

₹

$$\frac{\Phi}{\mathcal{E}}$$

10

\$ 1268.00

---

\$

1

\$

§

\$

¢

\$

d. ☐ Fees are to be charged to a credit card. **WARNING:** Information on this form may become public. **Credit card information should not be included on this form.** Provide credit card information and authorization on PTO-2038.

SEND ALL CORRESPONDENCE TO:

**SIGNATURE**

AJIT K. ZACHARIAS

NAME \_\_\_\_\_

REGISTRATION NUMBER

10/089756

5

10

**SECURE MULTI-APPLICATION CARD SYSTEM****REFERENCE TO RELATED APPLICATIONS**

This patent application claims priority based on United States Provisional Patent Application Serial No. 60/159,491, entitled  
15 "Supracard" filed by the same inventor on October 15, 1999.

**TECHNICAL FIELD**

This invention relates to electronic transaction systems including credit cards, debit cards, and the like. More specifically, the invention  
20 relates to a multi-application card and associated transaction processing system for providing secure access to multiple card accounts.

**BACKGROUND ART**

Financial institutions and commercial companies issue credit and  
25 debit cards to individuals, groups of individuals, associations and businesses. In addition, people carry a variety of other types of cards including frequent flyer cards, video club cards, library cards, insurance cards and a driver's license. A quick count of the cards in one's wallet reveals how widespread this proliferation of cards has become. Typically,

consumers carry numerous cards and accept the inconvenience of bulging wallets.

Even if the annoyance of carrying multiple cards and finding the right card when needed is ignored, a greater problem remains. By carrying numerous cards, the consumer exposes himself to a greater risk of loss or theft. Canceling and replacing lost or stolen credit cards, debit cards and charge cards can create substantial stress for the cardholder. The source of this stress may reside in remembering the lost cards, finding the appropriate account numbers, informing the card issuers and awaiting the issuance of replacement cards. Unauthorized use of a stolen card before cancellation may further exacerbate the stress a cardholder experiences.

Commercial institutions have developed various techniques aimed at reducing fraudulent transactions. Financial institutions, for example, have implemented a Personal Identification Number (PIN) system. This system requires that consumers enter a PIN into an automatic teller machine (ATM) before proceeding with a transaction. While the PIN system may partially reduce fraudulent purchases for debit cards, the application of this system does not cover the broad area of retail purchases. Many charge cards and credit cards only require the PIN when using an ATM, if at all. This poses a security risk to the cardholder because anyone with a lost or stolen card can charge purchases to the card account.

A more recent solution to the security issue is the smart card. While there are various types, most smart cards include an embedded microprocessor and memory that can store substantial cardholder information. This approach supposedly provides merchants more information when deciding if the consumer is the cardholder. Like the PIN system, smart cards partially address the security issue aimed at

reducing fraudulent purchases. However, other security concerns emerge such as (1) information on the smart card could be accessed by an unauthorized user (2) unauthorized users could still make purchases and (3) smart cards do not protect privacy. For example, storing  
5 information on the card enables anyone with the ability to display the contents of a card to learn information about the cardholder. Even if the smart card could be used as a multi-application card and addresses the issue of too many cards, the inherent security risks inhibit its widespread implementation.

10 Therefore, there is a need for a system that substantially reduces the number of cards that a cardholder must carry while increasing the security of card-based transactions.

#### DISCLOSURE OF INVENTION

15 The present invention meets the needs described above in a secure multi-application card system. With this system, consumers experience additional convenience by replacing numerous cards with a single multi-application card. This replacement can result in saving time by eliminating the search for the "right" card. Using the multi-application  
20 card also reduces the space needed by consumers for card storage. With the invented system, a cardholder can carry a single multi-application card, referred to as a "Supracard," and using a simple index, access and invoke the use of multiple cards issued by multiple issuers and serving multiple purposes. Thus, the cardholder can use multiple  
25 credit, debit and other non-encoded, magnetically-encoded, bar-coded and microprocessor based cards without having to carry each individual card.

The present invention also provides secure access to one or more card accounts. By storing the cardholder's record in a location remote

from the multi-application card, the invention removes relevant account information, such as account number and expiration date, from easy access by an unauthorized user. To further increase security, the remote database may not contain personal identification numbers of the stored  
5 cards. As a result, potential hackers of the database still may not get information needed to use the cards. The invention also includes a lock feature where the multi-application card may be automatically locked from future transactions in the event of predefined actions. As a further advantage, cardholder may purposefully lock the card to prevent future  
10 transactions.

Generally described, the invention includes a multi-application card for providing secure access to multiple cards and accounts. The multi-application card stores a readable identification number that corresponds to the card. The invention also includes a database located remotely  
15 from the card. The database correlates the identification number with a record associated with the card. The record contains a list of card types, card numbers and expiry dates in positions relative to their associated indexes. The invention also includes a translator that receives a transaction request, which includes the identification number read from  
20 the multi-application card and an index obtained from a source other than the multi-application card. The translator then uses the received identification number to access the corresponding record in the database, and uses the received index to retrieve the corresponding card account number and expiry date. The translator then transmits the card account  
25 number and expiry date to the originator of the transaction request.

In view of the foregoing, it will be appreciated that the secure multi-application card system improves over the drawbacks of prior systems. The specific techniques and structures employed by the invention to improve over the drawbacks of the prior systems and accomplish the

advantages described above will become apparent from the following detailed description of the embodiments of the invention and the appended drawings and claims.

## 5 BRIEF DESCRIPTION OF DRAWINGS

Fig. 1 is a diagram illustrating the creation and maintenance of an account for a multi-application card according to the present invention, which is explained in greater detail with reference to FIGS. 2-6.

Fig. 2 is a functional block diagram illustrating a system for  
10 increasing the security of card-based transactions using a multi-application card.

Fig. 3 is a logic flow diagram illustrating a method for conducting card-based transactions with increased security using the multi-application card illustrated in FIG. 2.

15 Fig. 4 is a logic flow diagram illustrating a subroutine for obtaining specific account information for the method illustrated in Fig. 3.

Fig. 5 is a logic flow diagram illustrating a method for completing a refund of a card-based transaction using the multi-application card illustrated in FIG. 2.

20 Fig. 6 is a logic flow diagram illustrating a method for conducting a transaction at an automatic teller machine using the multi-application card illustrated in Fig. 2.

## MODE(S) FOR CARRYING OUT THE INVENTION

25 The present invention may be embodied in a method and system for increasing the security of card-based transactions using a multi-application card, referred to hereinafter as a Supracard, to access one or more conventional card(s) issued by one or more card issuer(s). The term "Supracard number", as used herein, generally refers to the number

assigned to the multi-application card. The term "index", as used herein, generally refers to a code pointing to a specific entry within a list of card information entries pertaining to a Supracard Number. The term "card account number", as used herein, generally refers to the account number or reference number pertaining to a card whose parameters are stored in the database by the Supracard cardholder. Consequently, "card account numbers" may include accounts related to credit cards, debit cards, charge cards, insurance cards, and library cards and any other cards, whether they are non-encoded, magnetically encoded, bar-coded or microprocessor-based cards.

This system provides security and convenience in processing credit and debit cards and verifying the identity of a cardholder. With this system, a cardholder may carry a single multi-application card, a Supracard, yet have use of all his/her other cards by using a simple index number. Thus, the cardholder can use credit, debit and identity cards without having to carry them. The invention encompasses the Supracard and a computer system, including hardware, software and a database.

The Supracard is of a standard credit-card size and flexibility, and may be non-encoded, magnetically encoded or microprocessor-based. In an additional embodiment, it also has a bar code. The visible information on the card may include the cardholder's name, a photograph of the cardholder, a Supracard identification number and a bar code. The magnetic stripe contains the Supracard Number and conforms to the specifications of standards bodies such as the American Bankers Association (ABA) and the American National Standards Institute (ANSI). The magnetic information is recorded to enable it to be read by a standard credit card reader. The bar code allows it to be read by a bar code reader.



The Supracard could be described as a "card of cards." In this hierarchical system described herein, the Supracard is a primary card. All other cards (Visa, Mastercard, American Express, club membership cards, etc.) are referred to as sub-cards. Sub-card information including type, card account number, expiration date and (optionally) PIN code, pertaining to each of the sub-cards is stored in a computer database. The Supracard number serves as the key to the record within the database where information on its associated sub-cards is stored. The combination of the Supracard number and a cardholder-selected index, is used to locate individual sub-card information. Each Supracard also has its own PIN code.

Sub-cards could include credit cards, debit cards, department and specialty store cards, library cards, club membership cards, health insurance cards, and any other card, including smart cards and other microprocessor based cards. Each of these sub-cards may or may not have PINs associated with them. The PINs of the sub-cards are not required to be stored in the Supracard database. The Supracard system aids in processing card-based transactions by providing sub-card information in response to authorized inquiries.

Consumers wishing to use a Supracard would sign up for the service operated by an authorized Supracard System Operator (SSO). Each customer would be assigned a Supracard number and a PIN code, and be issued a Supracard. In the preferred embodiment, each Supracard holder will be issued at least two Supracards.

Supracard holders may enter and/or update their debit, credit and other card details in the Supracard database of the SSO, assigning a different index number to each one. They could do this using a computer, a telephone keypad or other wireless device, and the Internet or some other telecommunications media. If Supracard cardholders

prefer, they may simply phone in the details to representatives at the SSO and have them enter and maintain the sub-card information. Supracard holders may also designate one or more indexes as "Lock" indexes. If the Supracard is used with an index designated as a "Lock" index, access to pre-selected or all sub-card information will be locked. The lock may be removed by entering an index designated as an "Unlock" index.

At the time of purchase, if a consumer presents a Visa or Mastercard (or any credit, debit or identity card other than a Supracard), the charge authorization transaction is sent by the merchant system, received by a card processor's system and, based on the card Issuer Identification Number (IIN, part of the credit/debit card number) routed to the proper bank/financial institution's system for approval. However, if the IIN shows that it is a Supracard, the card processor's system recognizes that it needs the actual card number. If an index is not entered, the Supracard holder will be prompted for the index. The card processor's system receives the index selected by the Supracard holder, retains any PIN entered, and sends the Supracard number and the index to the SSO system. The SSO system, using the Supracard number and the index, extracts the selected card account number and expiration date from its database of pre-stored information, and sends them to the card processor's system. Now, using the actual card account number and expiration date (together with any entered PIN), the card processor's system routes the transaction to the proper bank/financial institution's system for approval or denial. When the card processor's system receives a response to the transaction from the bank/financial institution, it sends it to the merchant's terminal requesting authorization. Payment for the purchase will be credited to the merchant's account, less the

charges for the use of the credit/debit card and use of the Supracard, while the account pertaining to the sub-card is debited.

Credits and adjustments will be similarly handled. In case of refunds or adjustments, if a consumer presents a Visa or Mastercard (or  
5 any credit, debit or identity card other than a Supracard), the credit transaction is sent by the merchant system, received by the card processor's system and based on the card Issuer Identification Number (IIN, part of the credit/debit card number) routed to the proper bank/financial institution's system so that the credit is applied to the  
10 appropriate account. However, if the IIN shows that it is a Supracard, the card processor's system once again recognizes that it needs the actual card number. If an index is not entered, the Supracard holder will be prompted for the index. The card processor's system receives the index selected by the Supracard holder, retains any PIN code entered, and  
15 sends the Supracard number and the index to the SSO system. The SSO system, using the Supracard number and the index, extracts the selected card account number and expiration date from its database of pre-stored information, and sends them to the card processor's system. Now, using the actual card account number and expiration date (and any  
20 entered PIN code), the card processor's system routes the transaction to the proper bank/financial institution's system so that the credit can be applied to the appropriate account. When the card processor's system receives a response to the transaction from the bank/financial institution, it sends it to the merchant's terminal that initiated the transaction. The  
25 merchant's account is debited by the amount of the credit, subject to the adjustments for use of the credit/debit card and use of the Supracard, while the account pertaining to the sub-card is credited.

In the case of an ATM transaction, prior to permitting access to the bank's ATM functions, if a consumer uses a Bankcard, the transaction

proceeds normally. However, if it is a Supracard, the Bankcard system detects that the card used is a Supracard. The Supracard holder is prompted to enter the index pertaining to the Bankcard. The Bankcard system receives the index entered by the Supracard cardholder, and  
5 sends the Supracard number and the index to the SSO system. The SSO system, using the Supracard number and the index, extracts the selected card account number (in this case, the Bankcard number), and expiration date from its database of pre-stored information, and sends them to the Bankcard system. Now, using the actual Bankcard number  
10 and expiration date, the Bankcard system processes the transaction as it would normally.

From a security aspect, anyone stealing a Supracard will not even know what cards are registered on the Supracard, let alone the index codes to use them. Three false entries and the Supracard can be locked.  
15 The thief may also lock the card by unknowingly entering an index preset to "Lock" the card. In this case, the legitimate cardholder will not have to go through the laborious process of canceling all cards. Whether the Supracard is stolen or just lost, a spare Supracard will allow the user to instantly change the Supracard PIN code, and continue to use it.

20 Referring now to the drawings in which like numerals indicate like elements throughout several figures, FIG. 1 illustrates creation and maintenance of an account for a multi-application card, or Supracard, according to the present invention. At the time the Supracard account is created, a Supracard representative uses the Supracard control system  
25 **105** to complete setup tasks. These tasks may include ordering a Supracard, assigning a Supracard number and PIN, storing acquired cardholder information, creating a cardholder record **110** and storing a cardholder-selected login ID and password.

After creating the Supracard account, the Supracard representative may inform the cardholder that the account has been created. At this time, the cardholder may access his record **110** using one of the communication devices illustrated in FIG. 1. For example, a cardholder  
5 may connect to the Supracard system through the communication media **115** using the computer **120**, and modify his record. Alternatively, the cardholder may directly interact with a Supracard system and modify his record using the keypad of the telephone **125** or wireless device **130**.

Before allowing the cardholder access to his record, the Supracard  
10 control system **105** may request additional information. For example, the Supracard control system **105** may ask that the cardholder enter his login ID and password as previously defined. After authenticating the cardholder's identity, the cardholder may receive access to his record. At this point, the cardholder may add, modify or delete cards in his  
15 Supracard record in the database. For example, the cardholder may increase security by assigning all indexes between 20 and 50 as lock codes to increase the chance that a thief may use one of them and lock the card.

Alternatively, the cardholder may speak with and have a Supracard  
20 system representative modify his record using a computer or terminal connected to the Supracard control system **105**. In an alternative embodiment, the cardholder may review his spending statistics by looking at his transaction log. At the end of the record modification, the  
25 Supracard control system **105** updates the cardholder record accordingly.

Each cardholder record **110** includes an indexed table with entries relating to the corresponding cardholder's cards. While a record may include multiple cards, the invention is equally applicable to a single card record. As shown in the exploded view of Record "A" shown in FIG. 1,

entry 00 corresponds to the cardholder's American Express card with account number 289317568. Similarly, entries 36 and 99 correspond to the cardholder's Visa card with account number 327659000 and county library card with account number 52369, respectively. Although not shown, in addition to the Card Name and Account No., entries may contain expiry date, PIN numbers and other information pertaining to the sub-card. Typically, the index code corresponds to a two-digit number ranging from 00 to 99 selected by the cardholder. Alternative embodiments may include index codes of more or less digits or alphanumeric codes.

Entries 17 and 78 of Record A correspond respectively to lock and unlock indexes that add security as explained with reference to FIG. 2. Use of the lock index blocks the process of future transactions on the associated Supracard. In contrast, the unlock index can return the Supracard to a state that allows the process of future transactions. In an alternative embodiment, the Supracard control system 105 may block the process of future transactions after processing a designated number of erroneous index codes. In an alternative embodiment, the cardholder may purposefully invoke the lock and unlock features by selecting the corresponding index codes.

FIG. 2 is a functional block diagram illustrating a system 200 for increasing the security of card-based transactions using a multi-application Supracard 205. The Supracard 205 can replace various types of consumer cards including discount grocery cards, library cards, video rental cards, credit cards and debit cards. When a consumer decides to obtain, for the purpose of using, a Supracard, the system 200 assigns this consumer a Supracard number or identification number. Each Supracard number corresponds to a cardholder record 110 as explained with reference to FIG. 1. The Supracard 205 may include a

magnetic strip with the Supracard number encoded. Alternatively, the Supracard **205** may include a bar coded version of the Supracard number. The Supracard **205** may also include a picture **206** of the consumer. During a transaction, the merchant may compare the  
5 consumer's picture to the consumer before completing a transaction.

To begin a transaction, the merchant may scan the Supracard **205** using a keypad/card scanner **210**. By scanning the Supracard **205**, the merchant retrieves the Supracard number. The consumer enters the index of the card he desires. Typically, only the cardholder knows the  
10 correct indexes for the Supracard as defined in his cardholder record. As described with reference to FIG.1, the cardholder records include a lock index.

When a consumer enters a lock index, it begins a series of actions that denies the merchant authorization for the purchase. In addition, the  
15 system **200** may return an authorization denial if the consumer enters erroneous indexes a predefined number of times. Once locked, the Supracard **205** may only be unlocked by the cardholder by the record procedure explained with reference to FIG. 1. Consequently, the lock feature increases security with the multi-application Supracard **205**. For  
20 example, a cardholder that loses his Supracard **205** can quickly lock it. If an unauthorized user attempts fraudulent purchases before the cardholder realizes his Supracard is lost, the user's guessing at an index may also lock the card.

The merchant subsystem **215** receives both the Supracard number and index from the keypad/card scanner **210**. The merchant subsystem  
25 **215** manages the merchant's authorization request for the card issuer. Specifically, merchant subsystem **215** transmits the Supracard number and index to a card processor **220**, receives a response information from the remote card processor **220** and prints a corresponding invoice. One

5 The card processor **220** contacts the card issuers on behalf of the merchant. In a conventional credit card transaction, the card processor **220** simply contacts the card issuer for authorization. When a Supracard is used, the card processor **220** recognizes the need to retrieve the actual card account number; the card processor **220** forwards the  
10 Supracard number and index to the card translator **225**.

When the index entered by the consumer corresponds to a lock index, the database **225** may return a predefined message indicating that consumer entered an invalid index. As a result, the card translator **225** may designate the cardholder record as locked and transmit an “invalid code” message to the card processor **220**. In addition, the card translator **225** may deny future requests for the associated Supracard number and index combination until cardholder unlocks that card. The consumer may unlock the Supracard **205** as explained with reference FIG. 1.



If the card processor **220** does not receive the account number and expiration date from the card translator **225**, the card processor **220** can transmit a transaction denial to the merchant. This system avoids the card processor **220** involving the card issuer should the consumer enter an invalid index. Thus, fraudulent purchases may be denied quickly without involving the card issuer. When a consumer enters an undefined index, the system **200** may allow correction as explained with reference to FIG. 2.

After receiving the account number and expiration date from the card translator **225**, the card processor **220** transmits this information along with the transaction amount and other relevant control information to the appropriate issuer subsystem **235**. One skilled in the art will appreciate card processor **220** may also forward a PIN it may have received from merchant subsystem **215**. The issuer subsystem **235** reviews the received information and returns either an authorization or denial. The card processor **220** then returns the authorization or denial to the merchant subsystem **215**. The merchant subsystem **215** proceeds with the transaction accordingly.

The system **200** increases the security of card-based transactions by using the Supracard **205** in combination with the card translator **225** and database **230**. In alternative embodiments, the function of these devices may be housed in merchant subsystem **215**, card issuer subsystem **235**, Bankcard system (not shown) or card processor **220**. While FIG. 2 illustrates the implementation of the present invention with card-based purchases or rentals, the invention may also be used with refund transactions and requests to automated teller machines. These applications will be explained in greater detail with reference to FIGS. 5-6, respectively.

FIG. 3 is a logic flow diagram illustrating a method for conducting card-based transactions with increased security using the Supracard **205** illustrated in FIG. 2. In step **305**, a merchant scans the Supracard **205** for the Supracard number. Though not shown, the merchant completes the step **305** after the consumer requests a service or goods purchase. Step **305** is followed by step **310**, in which the merchant receives the index code entered by the consumer. Generally, the number entered by the consumer in this step is assumed to be the index even if the format is improper. For example, a fraudulent consumer may enter a four-digit number he suspects as the PIN number.

Step **310** is followed by step **315**, in which the merchant subsystem **215** transmits the entered index and Supracard number to the card processor **220**. However, the merchant subsystem **215** may also transmit additional information. For example, the merchant subsystem **215** could transmit a third number designated as the PIN if the selected sub-card requires a PIN. In an alternative embodiment, steps **305** through **310** may be combined with step **320**.

Step **315** is followed by step **320**, in which the card processor **220** determines if the received numbers correspond to a Supracard. The card processor **220** may be programmed to include additional code that can identify Supracards by their Issuer Identification Number. If the card processor determines that the received information corresponds to a Supracard, the "YES" branch is followed from step **320** to step **325**. In step **325**, the card processor **220** transmits the index and Supracard number to the card translator **225**. Step **320** is followed by subroutine **330**, in which card translator **225** obtains account information. Subroutine **330** will be described in greater detail with reference to FIG. 4.

Subroutine **330** is followed by step **333**, in which the card processor **220** determines if the card translator **225** transmitted the account information. In this step, the card processor **220** assesses if it possesses the information needed to proceed or if it should return a denial message  
5 to the merchant subsystem **215**. If the card processor received the account information, the "YES" branch is followed from step **333** to step **335**. If in step **320** the card processor **220** determines the scanned card is not a Supracard, the "No" branch is followed from step **320** to step **335**. In this step, the card processor **220** transmits the account information  
10 and transaction amount to the appropriate issuer subsystem **235**. To accomplish this, the card processor **220** identifies the appropriate card issuer using the account information received and an Issuer Identification Number. Because this identification process would be well known to one skilled in the art of card-based transactions, the details of this process is  
15 not repeated here.

Step **335** is followed by step **340**, in which the card processor **220** receives authorization from the issuer subsystem **235** for the requested transaction. The authorization may indicate that the transaction is either granted or denied. Step **340** is followed by step **345**, in which the card  
20 processor **220** transmits the received authorization to the merchant subsystem **215**.

If the "NO" branch is followed from step **333** to step **350**, the card processor **220** generates a transaction denial as explained with reference to FIG. 2. This denial could indicate that the information entered is  
25 incorrect and that the transaction has been cancelled. Step **350** is followed by step **355**, in which the card processor **220** transmits the transaction denial to the merchant subsystem **215**. Step **345** and step **355** are followed by the "END" step. At this point, the merchant has received information regarding the card transaction and can respond

accordingly. If the merchant received a denial, he may allow the consumer to enter the number again or alert authorities.

FIG. 4 is a logic flow diagram illustrating a subroutine **330** for obtaining account information for the method illustrated in FIG. 3.

5 Subroutine **330** begins from step **325** shown on FIG. 3. In step **405**, the card translator **225** identifies the cardholder record corresponding to the scanned Supracard number. To identify the appropriate cardholder record, the card translator **225** may utilize "look-up" tables. Step **405** is followed by step **410**, in which the card translator **225** retrieves account  
10 information from the database **230**. This retrieval may include the step of identifying the sub-card corresponding to the index. The account information may include the expiration date and account number.

Step **410** is followed by step **415**, in which the card translator **225** determines if it retrieved the desired account number. As described with  
15 reference to FIG. 3, a fraudulent consumer may enter an index not defined by the cardholder or a lock index. By completing step **410**, the card translator **225** may implicitly identify the validity of the index entered by the consumer. If the card translator **225** retrieved the account number, the "YES" branch is followed from step **415** to step **420**. In step  
20 **420**, the card translator **225** returns the account number and expiration date to the card processor **220**. Step **420** is followed by the "CONTINUE" step **425**, in which the subroutine **330** returns to step **333** shown on FIG. 3.

If the card translator **225** did not retrieve the account number, the  
25 "NO" branch is followed from step **415** to step **430**. Following the "NO" branch indicates that the index entered by the consumer either does not exist or corresponds to a lock/unlock index. Consequently, the card translator **225** updates the cardholder record to reflect this situation. One skilled in the art will appreciate that card translator **225** may store this

update in a status field. Updating the cardholder record may also include generating a denial message. Step 430 is followed by step 435, in which the card translator sends a denial message to the card processor 220. Step 435 is followed by the "CONTINUE" step 425, in which the  
5 subroutine 330 returns to step 333 shown on FIG. 3.

FIG. 5 is a logic flow diagram illustrating a method for completing a refund for a card-based transaction using the Supracard 205. Steps 505 through 525, subroutine 530, and steps 550 through 555 substantially resemble steps 305 through 325, subroutine 330, and steps 350 through  
10 355 explained with reference to FIG. 3. For the sake of brevity, that description will not be repeated here. Subroutine 530 is followed by step 535, in which the card processor 220, transmits both account and refund information to the appropriate issuer subsystem. Step 535 is followed by step 540, in which the card processor 220 receives confirmation from the  
15 issuer subsystem that the refund will be credited. Step 540 is followed by step 545, in which the card processor 220 transmits the confirmation response to the merchant subsystem 215.

Fig. 6 is a logic flow diagram illustrating a method for conducting a transaction at an automatic teller machine (ATM) using the Supracard  
20 205 illustrated in FIG. 2. In step 605, the ATM scans the card submitted by the consumer for the card number. Step 605 is followed by step 607, in which the merchant subsystem receives the entered index. Step 607 is followed by step 610, in which the ATM determines if the scanned card is a Supracard as described with reference to step 320 shown on FIG. 3.  
25 If the ATM identifies a Supracard in step 610, the "YES" branch is followed from step 610 to step 625.

In step 625, the ATM transmits the Supracard number and index to the card translator 225. Step 625 is followed by subroutine 630, in which the card translator 225 obtains account information as described with

reference to subroutine **330** of FIG. 3. Subroutine **630** is followed by step **635**, in which the ATM transaction is processed using conventional methods. In an alternative embodiment, transaction denials, as described with reference to FIGS. 3-4, could be implemented in an ATM transaction. For this embodiment, FIG. 6 could be modified to include additional steps.

The present system and method substantially reduces the number of cards that a cardholder must carry by using a multi-application Supracard **205**. Because the index is the primary limitation of the number of cards included in a cardholder record, a substantial number of cards currently carried may be reduced. In addition, the versatility of using either a standard card or bar code reader further demonstrates the widespread applicability. Moreover, the locking feature of the Supracard substantially improves a consumer's security risks, especially in retail settings. Finally, the accessibility of the cardholder's record further allows quick resolution in case the card is lost.

In view of the foregoing, it will be appreciated that present invention provides a method and system for increasing the security of card-based transactions using a multi-application card to access card issuers. It should be understood that the foregoing relates only to the exemplary embodiments of the present invention, and that numerous changes may be made therein without departing from the spirit and scope of the invention as defined by the following claims.

25

## AMENDED CLAIMS

[received by the International Bureau on 17 April 2001 (17.04.01);  
original claims 1-23 replaced by new claims 1-26 (8 pages)]

1. A system allowing a single cardlike device to be utilized in accessing  
5 a plurality of applications, the system comprising:  
a) a card processing system;  
b) a card reader communicatively coupleable to the card processing  
system, the card reader being operative to read a data  
identification number from the single cardlike device and to  
10 receive an index number through a data interface;  
c) the processing system, in response to receiving the data  
identification number and index number from the card reader,  
being operative to:  
i. identify an application associated with the data identification  
15 number and index when the index is within a first subset of the  
domain of potential index numbers;  
ii. disable the cardlike device from further use when the index is  
within a second subset of the domain of potential index numbers;  
and  
20 iii. re-enable a disabled cardlike device when the index is within  
a third subset of the domain of potential index numbers.
2. A system using a single cardlike device to access a plurality of  
applications, comprising:  
25 a) at least one card issuer subsystem;  
b) at least one card translator subsystem;  
c) a client subsystem, comprising:

i. a card reader, capable of reading data, including at least an identification number, from the cardlike device;

ii. a data entry means;

iii. means to:

5

1. read the identification number from the cardlike device;

2. determine whether the identification number needs to be translated to an account number;

3. prompt user to pre-select desired account number by entering its unique index using the data entry means;

10

4. send an account number request, including the identification number, together with the index, to a card translator subsystem;

5. receive a response to the account number request.

15

3. The system of claim 2, wherein the client subsystem is portable.

4. The system of claim 2, wherein the client subsystem is mobile.

5. The system of claim 2, wherein the index is at least one numeric character.

20

6. The system of claim 2, wherein the account number request is sent to a card processor subsystem that is operative to receive the request from any subsystem, process the request to determine that a card translator subsystem should receive the request, and transmit the request to the card translator subsystem.

25



- 29

1. receive an account number request including at least an identification number and an index;
  2. use the identification number and the index to retrieve account information pertaining to a single account number;
  3. when access to account information should be disabled, send a first response to the subsystem from which the account number request was received;
  4. when access to account information should be re-enabled, send a second response to the subsystem from which the account number request was received;
  5. when access to the account information should be denied, send a third response to the subsystem from which the account number request was received; and
  6. when access to the account information is permitted, send a fourth response including information pertaining to the single account, the information including at least the account number, to the subsystem from which the account number request was received.
11. The system of claim 10, wherein the account number request is received by the card translator subsystem from a card processor subsystem that is operative to receive a request from any subsystem, process the request to determine that the card translator subsystem should receive the request, and transmit the request to the card translator subsystem.
  12. The system of claim 10, wherein the account number request is received by the card translator subsystem from a card processor

subsystem that is operative to transmit the request including an identification number, together with an index, to the card translator subsystem.

- 5        13. The system of claim 10, wherein the account number request is received by the card translator subsystem from a card issuer subsystem that is operative to receive a request from any subsystem, process the request to determine that the card translator subsystem should receive the request, and transmit
- 10        the request to the card translator subsystem.
14. The system of claim 10, wherein the account number request is received by the card translator subsystem from a card issuer subsystem that is operative to transmit the request including an
- 15        identification number, together with an index, to the card translator subsystem.
15. The system of claim 10, wherein the account number request disables access to account information for future requests that
- 20        include the identification number.
16. The system of claim 10, wherein the account number request re-enables access to account information for future requests that include the identification number.
- 25        17. The system of claim 10, wherein the response to the account number request is received by a card processor subsystem, the card processor subsystem operative to receive the response,

process the response and transmit a response to the subsystem that initiated the account number request.

- 5 18. The system of claim 10, wherein the response to the account number request is received by a card issuer subsystem, the card issuer subsystem operative to receive the response, process the response and transmit a response to the subsystem that initiated the account number request.
- 10 19. The system of claim 10, wherein the index is at least one numeric character.
- 15 20. The system of claim 10, wherein the translator and database are stored in a system selected from the group comprising a client system, card processor system and card issuer system.
21. A method for secure processing of multi-application card transactions, comprising the steps of:
- 20 a) reading an identification number from a cardlike device;
- b) determining whether the identification number needs to be translated to an account number;
- c) accepting an index, pertaining to a single account number, using a data entry means;
- 25 d) sending an account number request, including the identification number, together with the index, to a card translator subsystem;
- e) using the identification number and the index, retrieving account information pertaining to the single account number;

- 5
- f) based on the index selected, disabling access to account information for future requests that include the identification number;
- g) based on the index selected, re-enabling access to account information for future requests that include the identification number;
- h) based on the index selected, receiving a response including at least the account number, pertaining to the pre-selected desired account.
- 10
22. The method of claim 21, further including sending the account number request to a card processor subsystem that is operative to receive a request from any subsystem, process the request to determine that the card translator subsystem should receive the request, and transmit the request to the card translator subsystem.
- 15
23. The method of claim 21, further including an account number request sent from a card processor subsystem that is operative to transmit the request including an identification number, together with an index, to a card translator subsystem.
- 20
24. The method of claim 21, further including sending the account number request to a card issuer subsystem that is operative to receive a request from any subsystem, process the request to determine that the card translator subsystem should receive the request, and transmit the request to the card translator subsystem.
- 25

5

26. A computer controlled apparatus operable for performing the method of claim 21.

## AMENDMENT

Kindly add new claim 27 as follows:

27. A method allowing a single cardlike device to be utilized in accessing a plurality of applications, the method comprising the steps of:
- a) reading a data identification number from the single cardlike device;
  - b) receiving an index number through a data interface;
  - c) identifying an application associated with the data identification number and the index number when the index number is within a first subset of the domain of potential index numbers;
  - d) disabling the cardlike device from further use when the index number is within a second subset of the domain of potential index numbers; and
  - e) re-enabling a disabled cardlike device when the index number is within a third subset of the domain of potential index numbers.

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization  
International Bureau



(43) International Publication Date  
26 April 2001 (26.04.2001)

PCT

(10) International Publication Number  
**WO 01/29789 A1**

(51) International Patent Classification<sup>7</sup>: G07F 7/02, 7/08

(21) International Application Number: PCT/US00/27584

(22) International Filing Date: 4 October 2000 (04.10.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:  
60/159,491 15 October 1999 (15.10.1999) US

(71) Applicant and

(72) Inventor: ZACHARIAS, Ajit, K. [CA/US]; 7375 Brassfield Drive, Cumming, GA 30041-8391 (US).

(74) Agent: ZACHARIAS, Ajit, K.; 7375 Brassfield Drive, Cumming, GA 30041-8391 (US).

(81) Designated States (national): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ,

DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States (regional): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

**Published:**

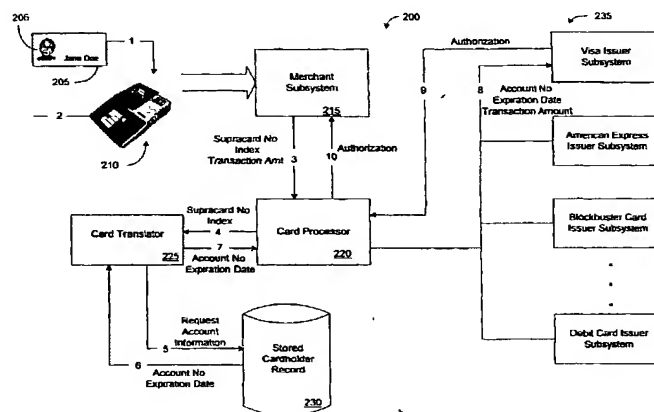
- With international search report.
- With amended claims and statement.

**Date of publication of the amended claims and statement:**

7 June 2001

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: SECURE MULTI-APPLICATION CARD SYSTEM



(57) Abstract: A multi-application card for providing secure access to multiple card accounts. This system includes a multi-application card storing a readable identification number corresponding to the card, and a database located remotely from the card. The database correlates the identification number with a record associated with the card, and the record contains a list of card account numbers and associated indexes. The system also includes a translator that receives a transaction request including the identification number read from the multi-application card and one of the associated indexes obtained from a source other than the card. The translator then uses the received identification number to access the corresponding record in the database, and uses the received index number to retrieve the corresponding card account number and expiry date. The translator then transmits the card account number and expiry date in response to the transaction request. With this system, a cardholder can carry a single multi-application card that provides access to multiple accounts associated with different cards by using a simple index. Thus, the cardholder can use multiple credit, debit and other non-encoded, magnetically encoded, bar-coded and microprocessor based cards, without having to carry each individual card.

WO 01/29789 A1



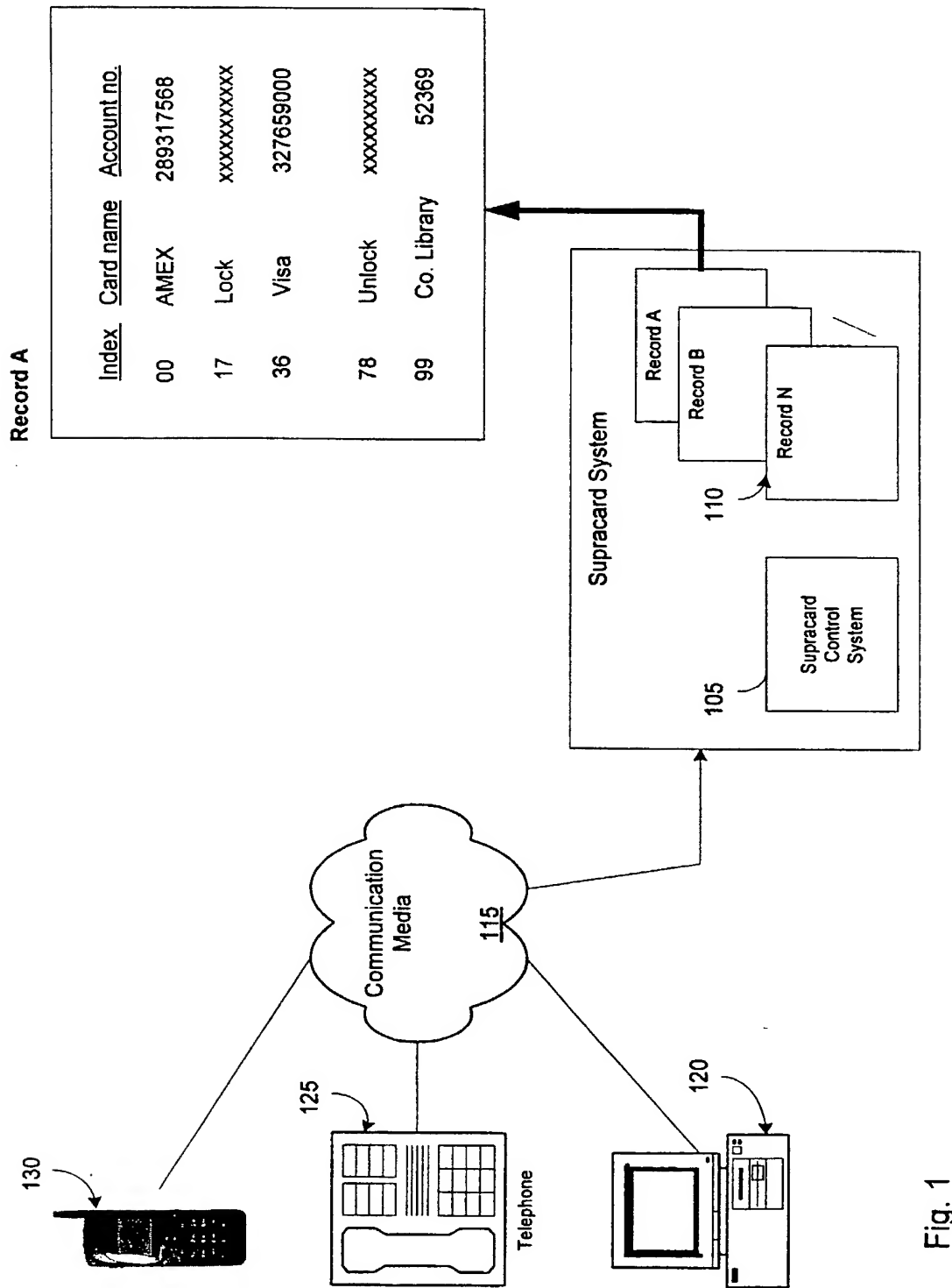


Fig. 1

10/089756

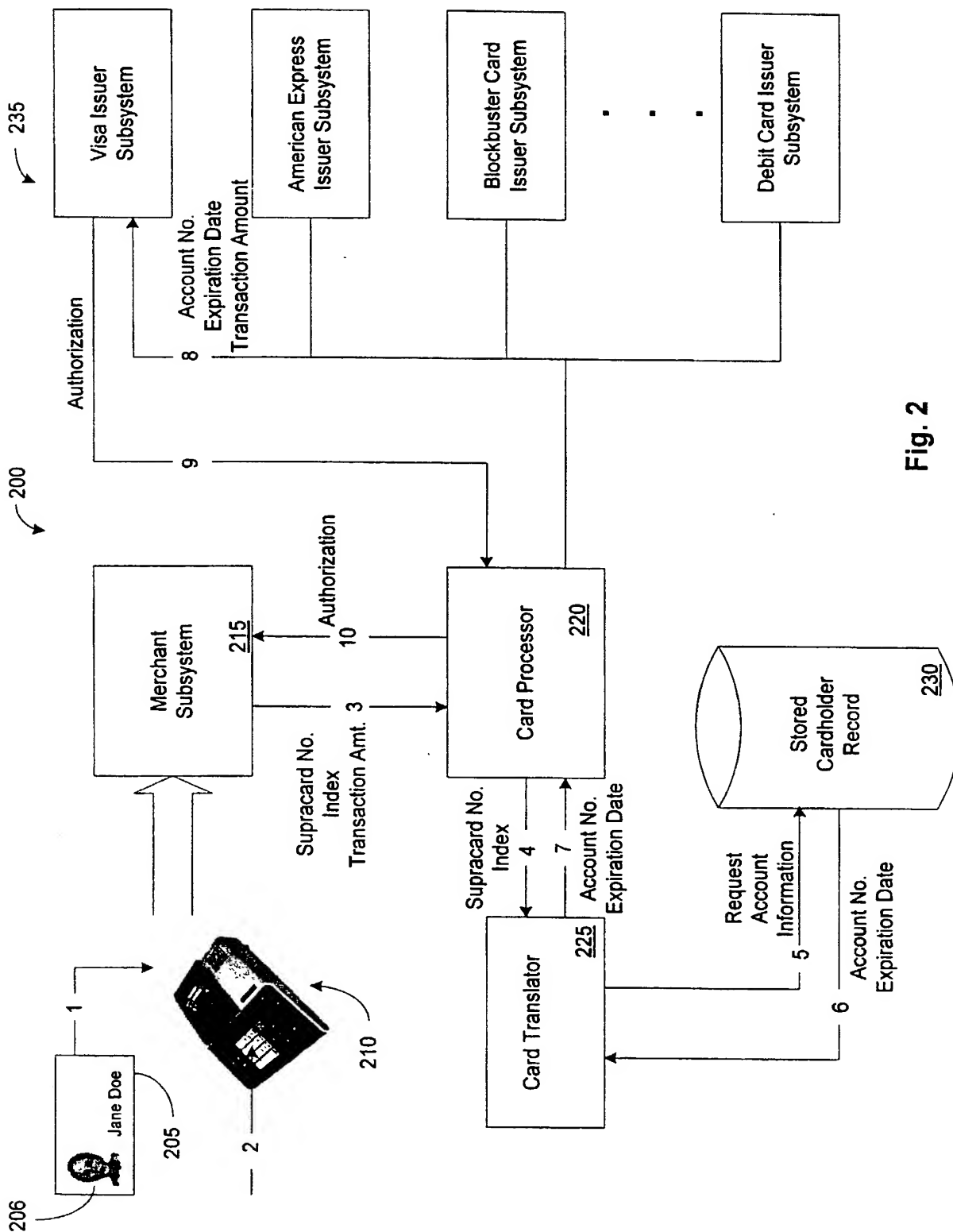


Fig. 2

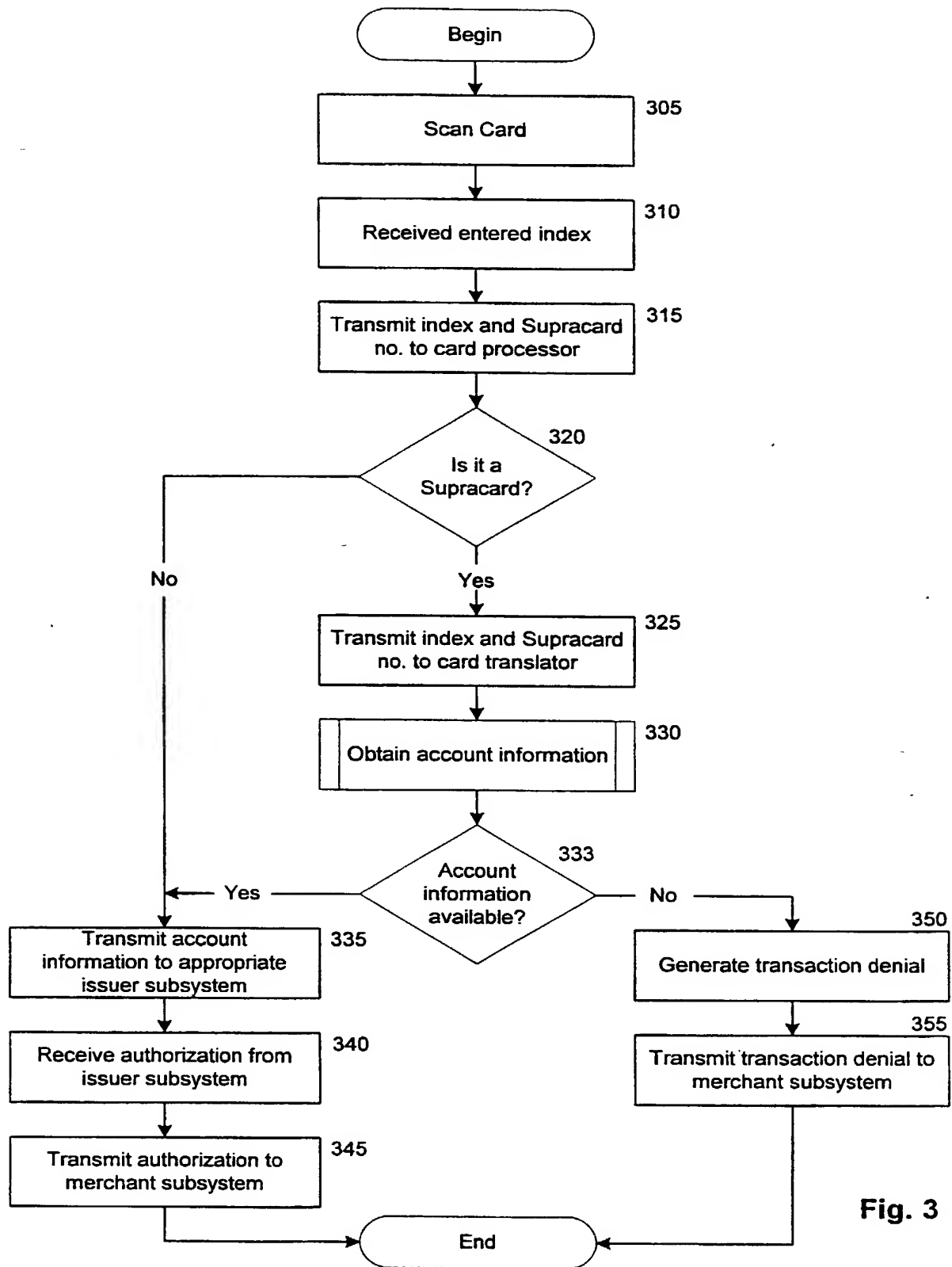


Fig. 3

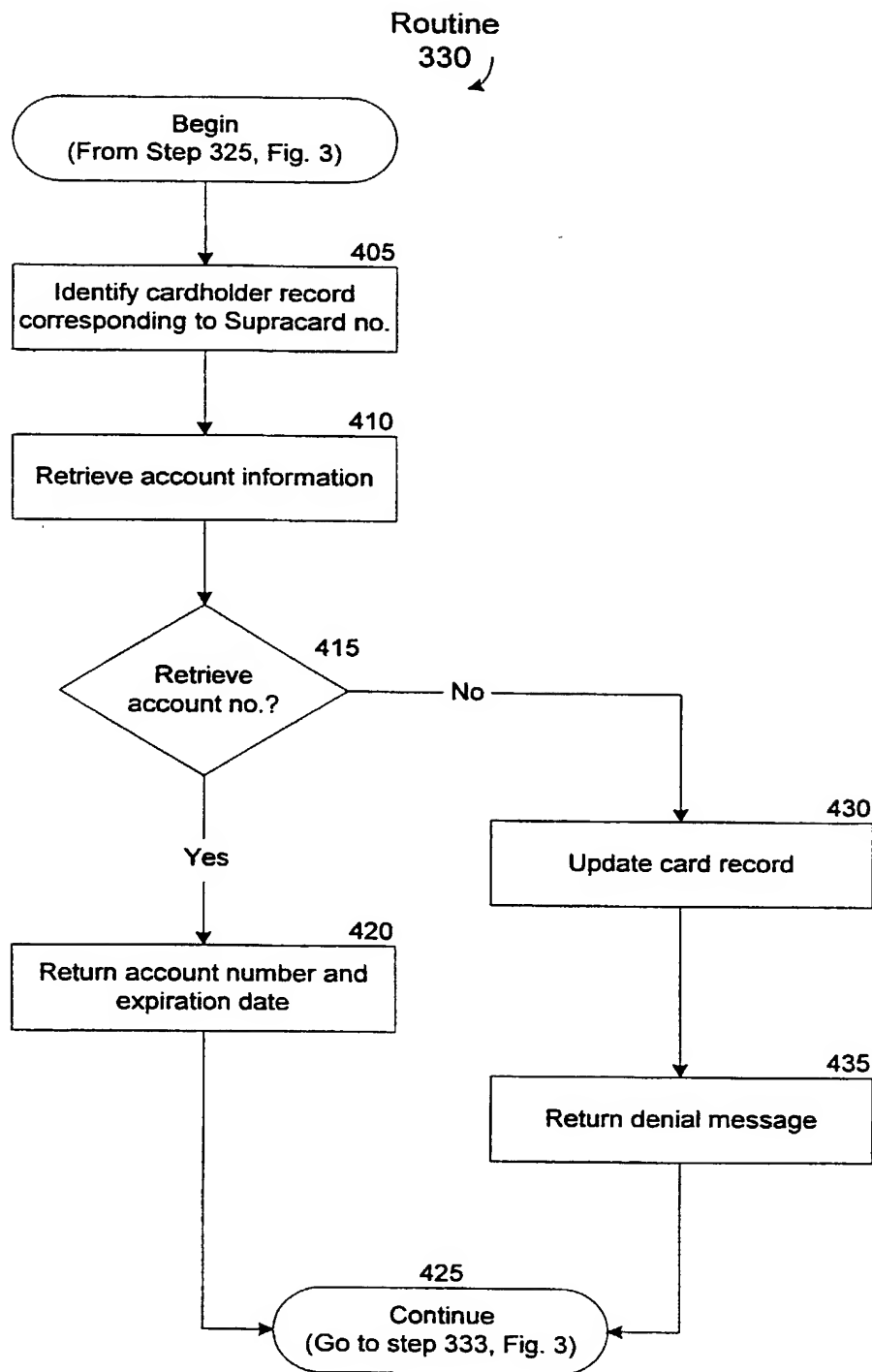


Fig. 4

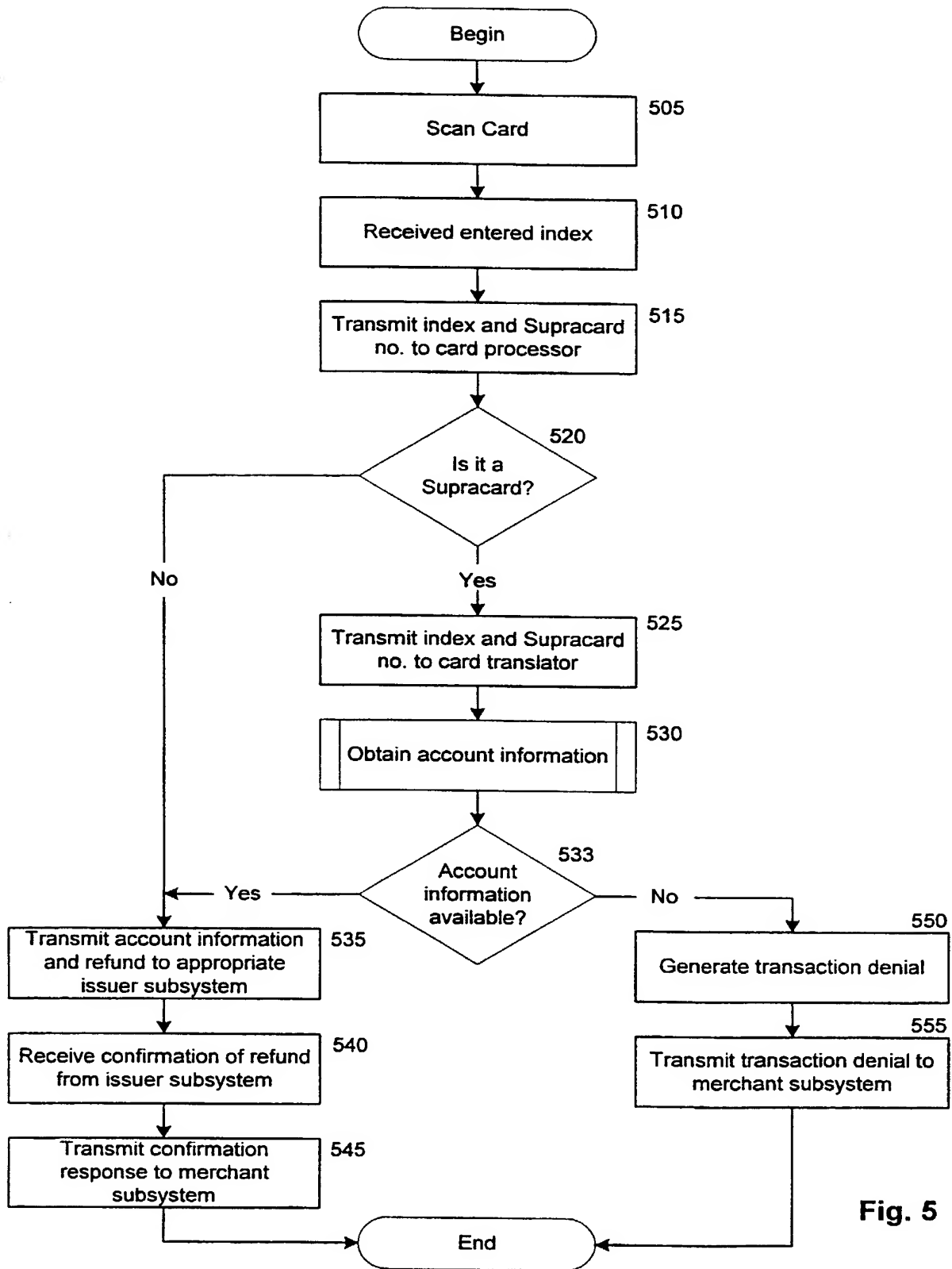


Fig. 5

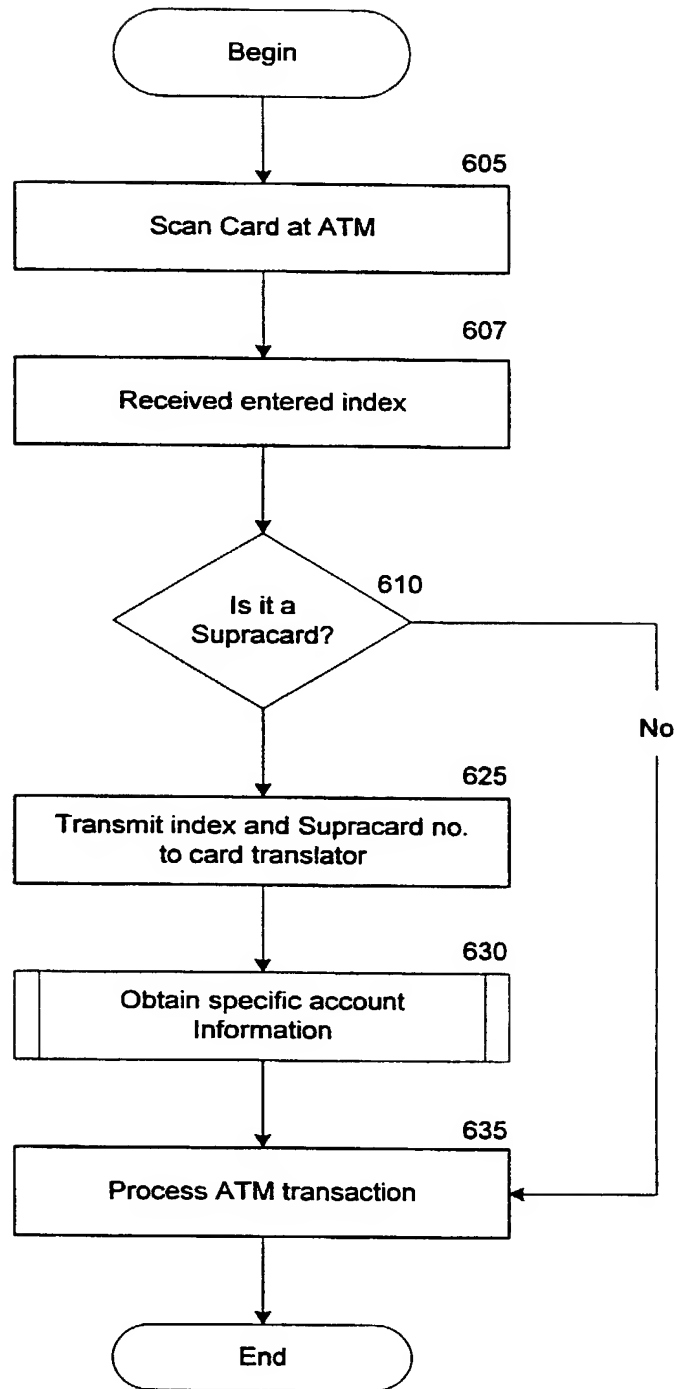


Fig. 6

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number

**DECLARATION FOR UTILITY OR  
DESIGN  
PATENT APPLICATION  
(37 CFR 1.63)**

☒ Declaration Submitted with Initial Filing      OR      ☐ Declaration Submitted after Initial Filing (surcharge (37 CFR 1.16 (e)) required)

Attorney Docket Number	AZSI - P - 010
First Named Inventor	AJIT K. ZACHARIAS
COMPLETE IF KNOWN	
Application Number	PCT/US00/27584
Filing Date	04 OCTOBER, 2000
Art Unit	
Examiner Name	

As the below named inventor, I hereby declare that:

My residence, mailing address, and citizenship are as stated below next to my name.

I believe I am the original and first inventor of the subject matter which is claimed and for which a patent is sought on the invention entitled:

SECURE MULTI-APPLICATION CARD SYSTEM

(Title of the Invention)

the specification of which

☐ is attached hereto

OR

☒ was filed on (MM/DD/YYYY) 10/04/2000 as United States Application Number or PCT International

Application Number PCT/US00/27584 and was amended on (MM/DD/YYYY) 04/17/2001 (if applicable).

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment specifically referred to above.

I acknowledge the duty to disclose information which is material to patentability as defined in 37 CFR 1.56, including for continuation-in-part applications, material information which became available between the filing date of the prior application and the national or PCT international filing date of the continuation-in-part application.

I hereby claim foreign priority benefits under 35 U.S.C. 119(a)-(d) or (f), or 365(b) of any foreign application(s) for patent, inventor's or plant breeder's rights certificate(s), or 365(a) of any PCT international application which designated at least one country other than the United States of America, listed below and have also identified below, by checking the box, any foreign application for patent, inventor's or plant breeder's rights certificate(s), or any PCT international application having a filing date before that of the application on which priority is claimed.

Prior Foreign Application Number(s)	Country	Foreign Filing Date (MM/DD/YYYY)	Priority Not Claimed	Certified Copy Attached?	
				YES	NO
			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

☐ Additional foreign application numbers are listed on a supplemental priority data sheet PTO/SB/02B attached hereto:

[Page 1 of 2]

Burden Hour Statement: This form is estimated to take 21 minutes to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, U S Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231.

**DECLARATION — Utility or Design Patent Application**Direct all correspondence to: ☐ Customer Number  OR ☒ Correspondence address below

Name

AJIT K. ZACHARIAS

Address

32 MERLIN DRIVE

City

BRAMPTON

State

ONTARIO

ZIP

L6P 1G1

Country

CANADA

Telephone

(905) 794-2752

Fax

(905) 794-1411

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under 18 U.S.C. 1001 and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

NAME OF SOLE OR FIRST INVENTOR:

☐ A petition has been filed for this unsigned inventorGiven Name  
(first and middle [if any])

AJIT KUMAR

Family Name  
or Surname

ZACHARIAS

Inventor's  
Signature

A.K. Zacharias

April 3, 2002  
Date

Residence: City

BRAMPTON

State

ON.

CANADA  
CountryCANADIAN  
Citizenship

Mailing Address

32 MERLIN DRIVE

CAN

City

BRAMPTON

State

ON.

ZIP

L6P 1G1

Country

CANADA

NAME OF SECOND INVENTOR:

☐ A petition has been filed for this unsigned inventorGiven Name  
(first and middle [if any])Family Name  
or SurnameInventor's  
Signature

Date

Residence: City

State

Country

Citizenship

Mailing Address

City

State

ZIP

Country

☐ Additional inventors are being named on the \_\_\_\_\_ supplemental Additional Inventor(s) sheet(s) PTO/SB/02A attached hereto.